Multitenant Architecture: Securing Splunk To Combat Snooping Users

HELPnet Technology Services

A division of Indiana University Information Technology Services

.conf2016

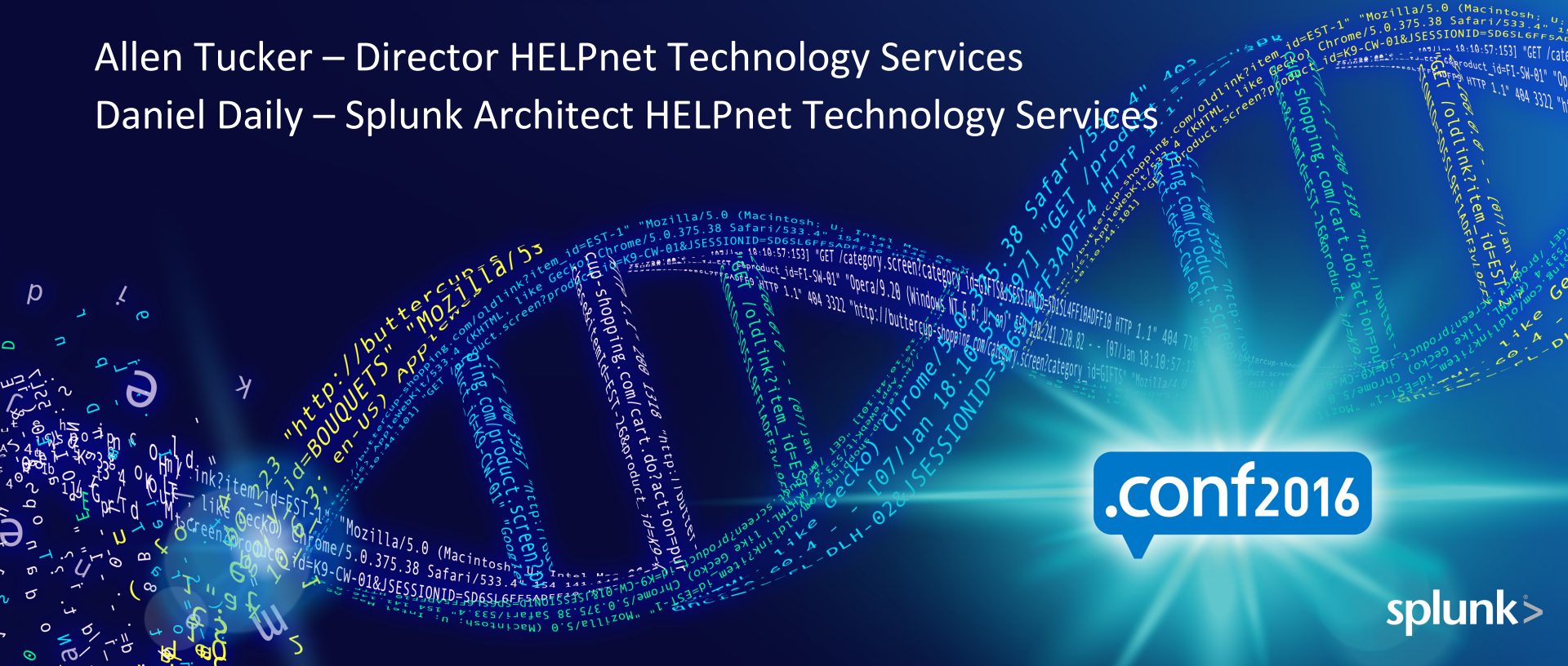
splunk>

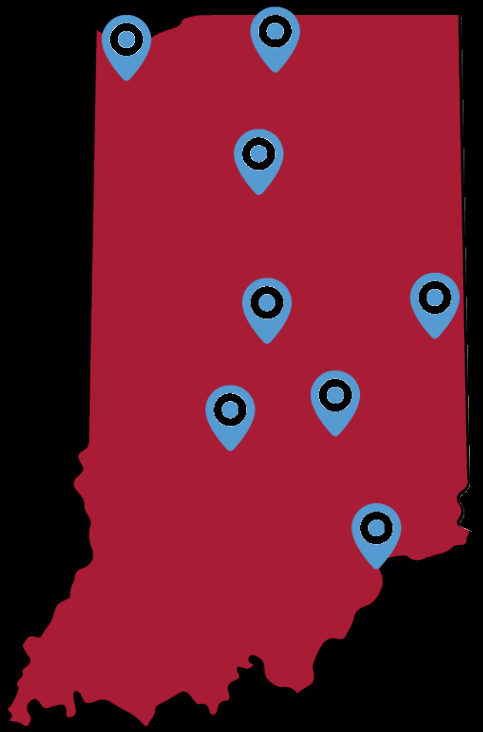
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Introduction

Allen Tucker – Director HELPnet Technology Services
Daniel Daily – Splunk Architect HELPnet Technology Services





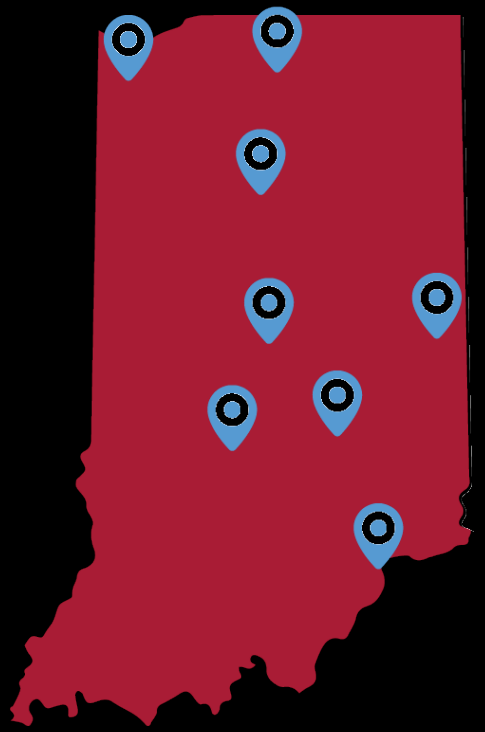
Indiana University, *est. 1820*

- **$3.3B** Enterprise
- Partnered with **$6B** IU Health system

- **115,000** Students
- **1.3M** Credit Hours per semester
- **>20,000** Degrees per year
- **$1.1B** In Financial Aid
- **$450M** In research grants

- **8,000** Acres
- **882** Buildings, 36M square feet
- **>600,000** *Living* Alumni

- **10,500** Faculty and Staff



CENTRALIZED enterprise I.T.
with
DECENTRALIZED departmental I.T.

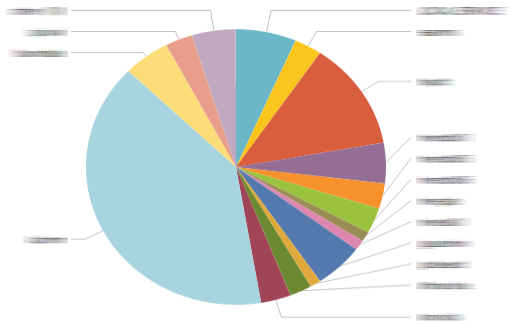
109 Departmental IT Groups
5213 Total Servers within IU

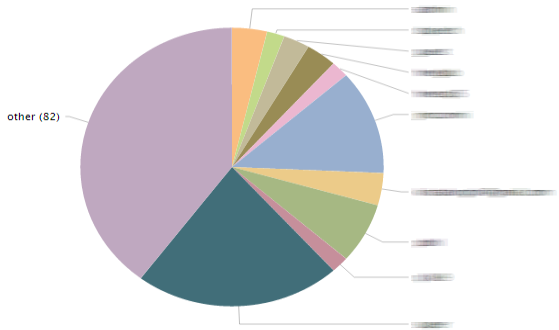
Safeguards

- IU I.T. Policy
  - IT-12 List of ‘best practices’ for system management
- IU Internal Audits
  - In depth departmental checks for IT operations
  - Alignment with IT policies
- Log management in IT-12
  - Success/Failed User Logons, Success/Failed File Accesses

Implications

- Costs associated with log review
  - Its overwhelming
    - Different log sources,
    - many servers
    - TONs of logs.
  - Costly if departments DIY
  - Staff time is at a premium
    - Admins can make much better use of your time being impactful to their departments





Failed File Access Total

	logon	host	count	total
1			135	135
2			43	43
3			22	22
4			1	18
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	
			1	

Failed User Logons Total

logon	host	count	total
		47	47
		26	26
		15	15
		8	8
		8	8

« prev 1 2 3 4 5 6 7 8 9 10 next »

Failed File Access

Notice: All boxes must contain at least one selection.

User	Host	File Path	Exclude Logon	Exclude Host	Exclude File Path		
[redacted]	All	*	NONE	NONE	NONE	Last 24 hours	Submit

<1m ago

Time	Host	User	File Path	Raw Log
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015516 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: SYNCHRONIZE ReadData (or ListDirectory) ReadAttributes Access Reasons: SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadAttributes: Granted by ACE on parent folder D:(A;OICIID;FA;;;S-1-5-21-1085031214-1292428093-527237240-83581) Access Mask: 0x100081 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015515 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: SYNCHRONIZE ReadData (or ListDirectory) ReadAttributes Access Reasons: SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadAttributes: Granted by ACE on parent folder D:(A;OICIID;FA;;;S-1-5-21-1085031214-1292428093-527237240-83581) Access Mask: 0x100081 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015514 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015513 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015512 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015511 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015510 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015509 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Favorites\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015508 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Favorites\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015	[redacted]	[redacted]	D:\Redirects\IU-	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info

Multitenant

- Not just the security team logging in
- Useful and meaningful apps, but they don't all pertain to everyone

Cas/Shib

This Dashboard shows all information for Cas/Shib

CAS Tickets per month trending over the past year

2,365,071 Tickets -9,477,315

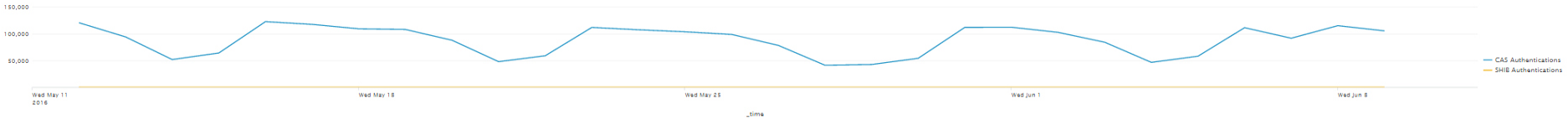
CAS Authentications for the last 12 months

8,838,078 Authentications

Shibboleth Authentications for the past 12 months

2,967,010 Authentications

Cas and Shib Authentications for the month



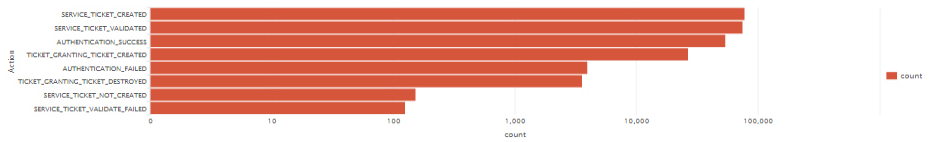
Failed Authentication Count by Location for the last 4 hours

Failed Authentication Attempts in the Last 4 hours by Client IP

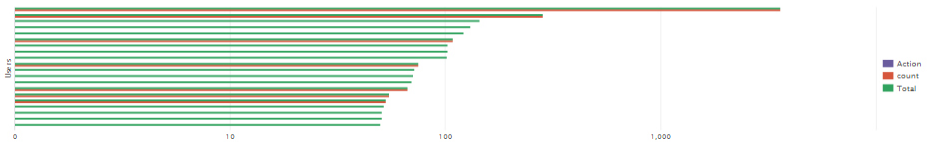
client_ip	City	Country	Region	lat	lon	count
[redacted]	Huntington	United States	Indiana	40.88310	-85.49750	22
[redacted]	Indianapolis	United States	Indiana	39.76840	-86.15800	12
[redacted]	Indianapolis	United States	Indiana	39.88540	-85.97380	12
[redacted]	Brick Township	United States	New Jersey	40.07070	-74.11080	11
[redacted]	Indianapolis	United States	Indiana	39.78510	-86.16650	9
[redacted]	Bloomington	United States	Indiana	39.24990	-86.45550	9
[redacted]	Indianapolis	United States	Indiana	39.82270	-86.14500	9
[redacted]		Uganda		1.00000	32.00000	9
[redacted]	Naperville	United States	Illinois	41.77010	-88.14040	8
[redacted]	Indianapolis	United States	Indiana	39.80980	-86.10100	8

« prev 1 2 3 4 5 6 7 8 9 10 next »

CAS Actions taken over the last 4 hours



Number of Actions taken by CAS Users over the last 4 hours

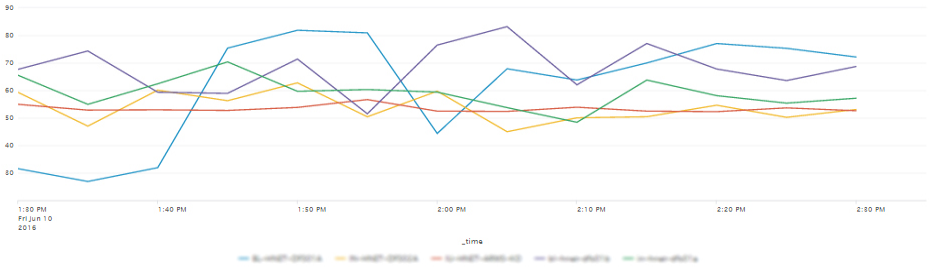


HELPnet IT Ops

Last 60 minutes

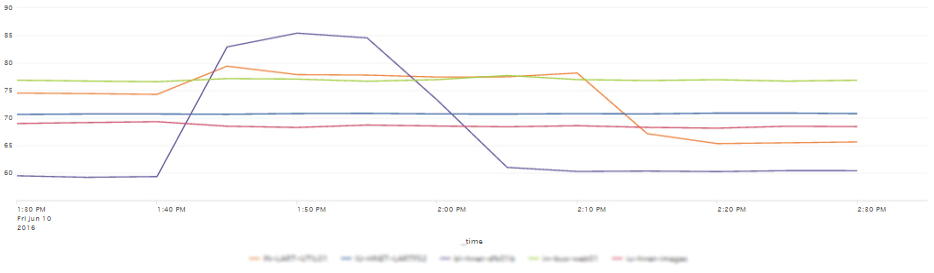
CPU - % Utilization

Top 5 Results - 1min Refresh



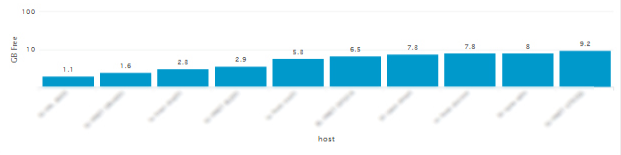
Memory - % Committed

Top 5 Results - 1min Refresh



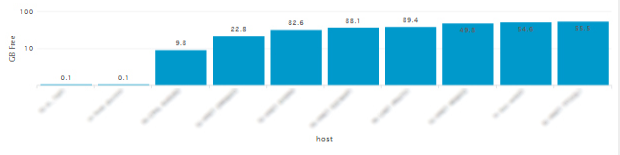
C: Drive - Free Space by GB

Lowest 10 Results - Last 15min - 15min Refresh



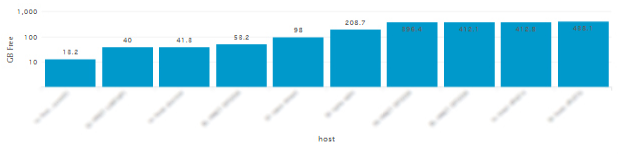
D: Drive - Free Space by GB

Lowest 10 Results - Last 15min - 15min Refresh



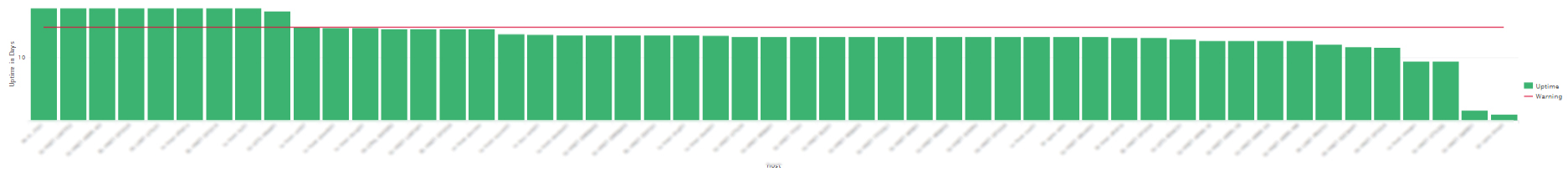
E: Drive - Free Space by GB

Lowest 10 Results - Last 15min - 15min Refresh



Up Time by Server

Last 60 Minutes



Antivirus Scan Status

30 day window

By Status by Time

host	Time	Detail	Scan_Parameters	Scan_Time	Status
[redacted]	06/10/16 12:01:20	Microsoft Antimalware scan has started.	Quick Scan	0:01:05	Scan Started
[redacted]	06/10/16 12:01:29	Microsoft Antimalware scan has started.	Quick Scan	0:01:35	Scan Started
[redacted]	06/09/16 12:03:18	Microsoft Antimalware scan has finished.	Quick Scan	0:02:11	Successful
[redacted]	06/09/16 12:03:39	Microsoft Antimalware scan has finished.	Quick Scan	0:02:02	Successful

Antivirus Engine Status

30 day window

By Status by Time

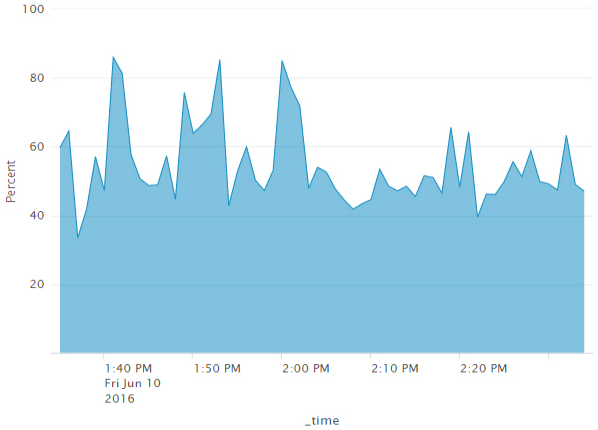
host	Time	Detail	Engine Version	Signature Version	Status
[redacted]	06/10/16 02:15:55	Microsoft Antimalware has encountered an error trying to update signatures. New Signature Version: Previous Signature Version: 1.223.1253.0 Update Source: Microsoft Update Server Update Stage: Search Source Path: http://www.microsoft.com Signature Type: AntiVirus Update Type: Full User: NT AUTHORITY\SYSTEM Current Engine Version: Previous Engine Version: 1.1.12805.0 Error code: 0x80248014 Error description: An unexpected problem occurred while checking for updates.	2.1.12706.0	116.3.0.0	*FAILED UPDATE*
[redacted]	06/10/16	Microsoft Antimalware Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.	1.1.12805.0	1.223.1193.0	Configuration

HELPnet IT Ops - Server

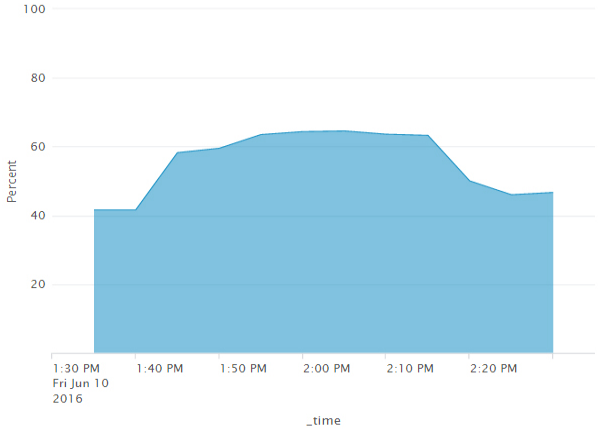
Server [redacted] Real-time Submit

Up Time	C: Drive - Free Space	D: Drive - Free Space	E: Drive - Free Space
14.51 Days	16.69 GB	1,521.27 GB	597.61 GB

Processor - % Utilization



Memory - % Committed



Antivirus Scan Status

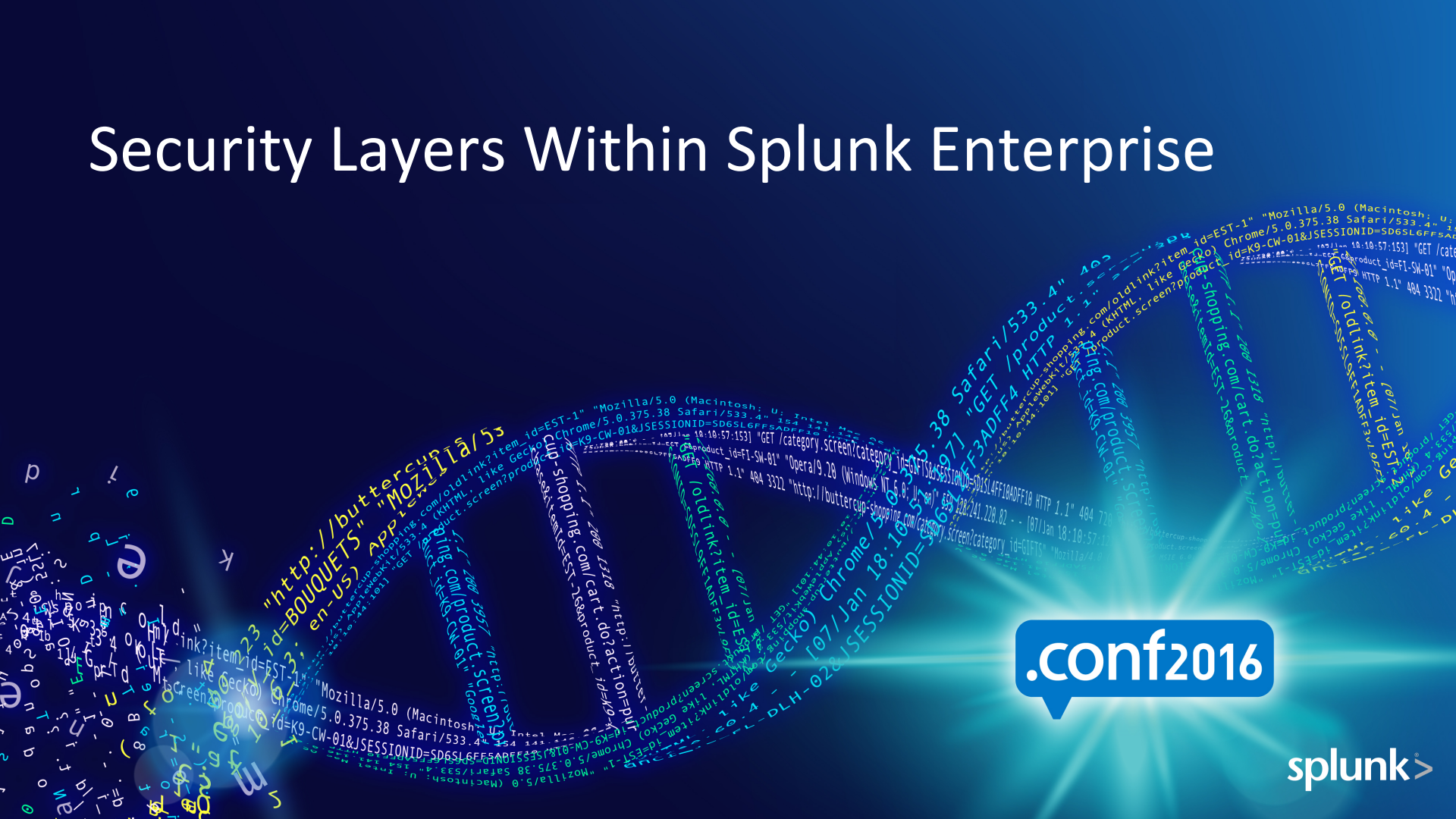
Scan Status

Time	Detail	Scan_Parameters	Scan_Time	Status
06/10/16 12:03:14	Microsoft Antimalware scan has finished.	Quick Scan	0:01:51	Successful

Engine Status

Time	Detail	Engine Version	Signature Version	Status
06/10/16 02:00:50	Microsoft Antimalware signature version has been updated.	1.1.12805.0	1.223.1193.0	Signatures Updated

Security Layers Within Splunk Enterprise



- **Index Layer**

Read Access

- Limit searchable data based on index
- Role based configurations

Application Layer

Read/Write Access

Views

Reports

Eventtypes

Role Based Configurations

authentication.conf

```
[iuhelpnet01]
SSLEnabled = 1
anonymous_referrals = 1
bindDN =
bindDNpassword =
charset = utf8
emailAttribute = mail
groupBaseDN = groupMappingAttribute = distinguishedname
groupMemberAttribute = member
groupNameAttribute = cn
host =
nestedGroups = 1
network_timeout = 20
port = 636
realNameAttribute = displayname
sizelimit = 1000
timelimit = 15
userBaseDN =
userNameAttribute = samaccountname
```

```
[roleMap_iuhelpnet01]
test = IU-UITS-SPLUNK-TEST
```

Role Based Configurations

authorize.conf

```
[role_test]
search = enabled
srchIndexesAllowed = _internal
srchIndexesDefault = _internal
srchJobsQuota   = 8
srchDiskQuota   = 250
accelerate_search = enabled
rest_properties_get = enabled
```

Index Layer Security Settings

authorize.conf

```
[role_test]
search = enabled
srchIndexesAllowed = _internal
srchIndexesDefault = _internal
srchJobsQuota   = 8
srchDiskQuota   = 250
accelerate_search = enabled
rest_properties_get = enabled
```

Capabilities

Select specific capabilities for this role.

Available capabilities — add all »

- accelerate_datamodel
- accelerate_search
- admin_all_objects
- change_authentication
- change_own_password
- delete_by_keyword
- edit_deployment_client

Selected capabilities — « clear all

- accelerate_search
- rest_properties_get
- schedule_rtsearch
- search

Indexes

Restrict this role's searches to the specified index(es). Search results for this role will only show events from these indexes.

Available search indexes — add all »

- All non-internal indexes
- All internal indexes
- _audit
- _internal
- _introspection
- _thefishbucket
- cas_summary
- firedalerts
- history
- iuhnet

Selected search indexes — « clear all

- _internal
- cas

Application Layer Settings

default.meta/local.meta

```
[]
access = read : [ admin, hnet, splunk-system-role ], write : [ admin ]
export = none

[reports]
access = read : [ admin, hnet, splunk-system-role ], write : [ admin ]
export = none
```

App permissions

Users with read access can only save objects for themselves, and require write access to be able to share objects with other users.

Roles	Read	Write
Everyone	☑	☐
admin	☐	☑
can_delete	☐	☐
cas	☐	☐
cne	☐	☐
cne-pci	☐	☐
denodo	☐	☐
hnet	☐	☐
iupc	☐	☐
iusb	☐	☐
iuse	☐	☐
kfs	☐	☐
nurs	☐	☐
power	☐	☑
splunk-system-role	☐	☐
test	☐	☐
user	☐	☐
windows-admin	☐	☐

Sharing for config file-only objects

Set permissions for configurations that have been copied over or added to config files rather than created through the UI. Objects defined in config files only (not in the UI) should appear in

◉ This app only (system) ○ All apps

Cancel Save

Shortcomings Of Single Layer Security Within Splunk

Limitations Of Only 1 Layer

Inclusive versus Exclusive

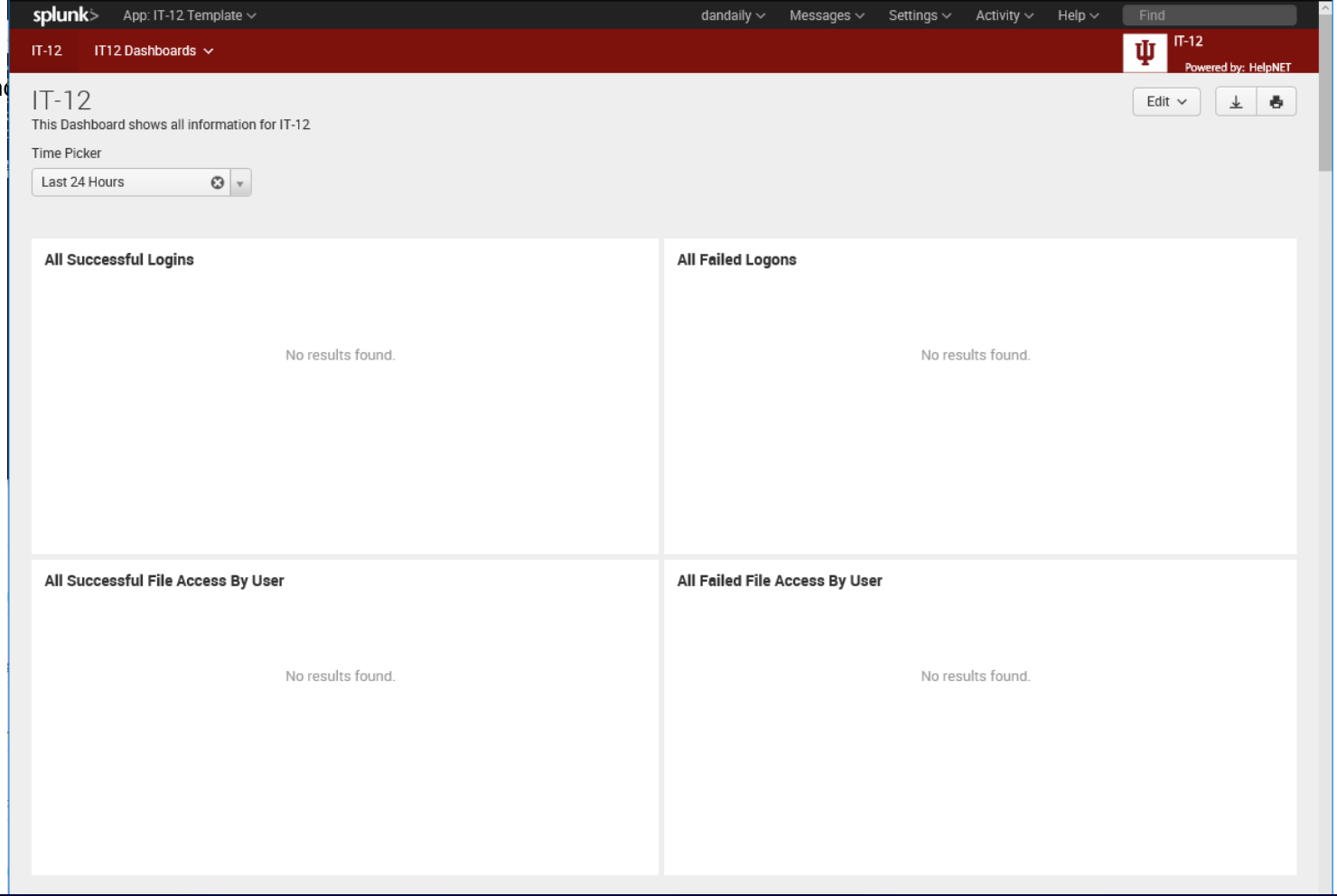
- Access to data pre
- Additional hoops t
- Users can intentio

urity loopholes

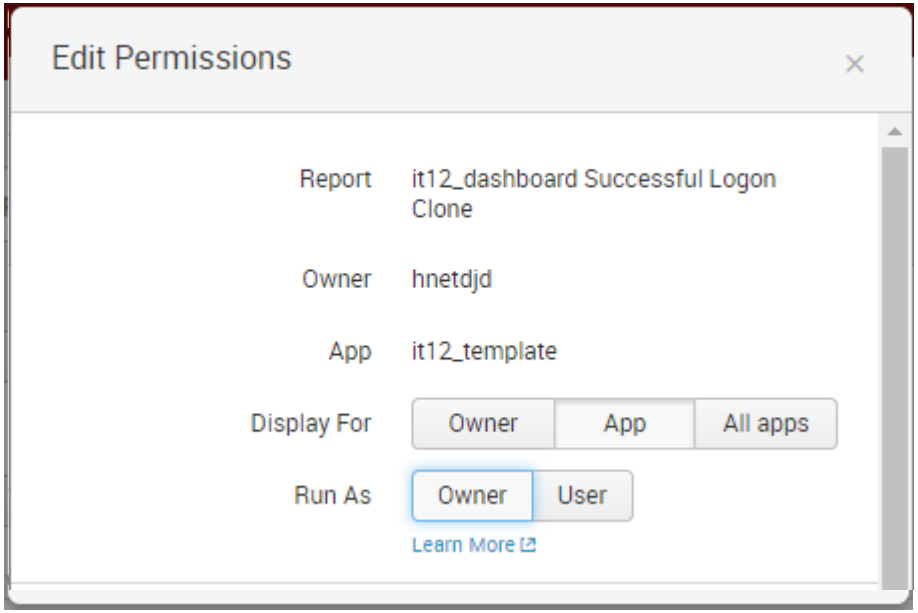
around the security

F.B.I. TERMINAL

This is a secured and monitored Federal Goverment system. Unauthorized access is strictly prohibited. All activity is fully monitored. Individuals who attempt to gain unauthorized access or attempt any modification of information on this sytem is subject to criminal prosecution. All persons who are hereby notified that use of this sytem constitutes concent to monitoring and auditing.



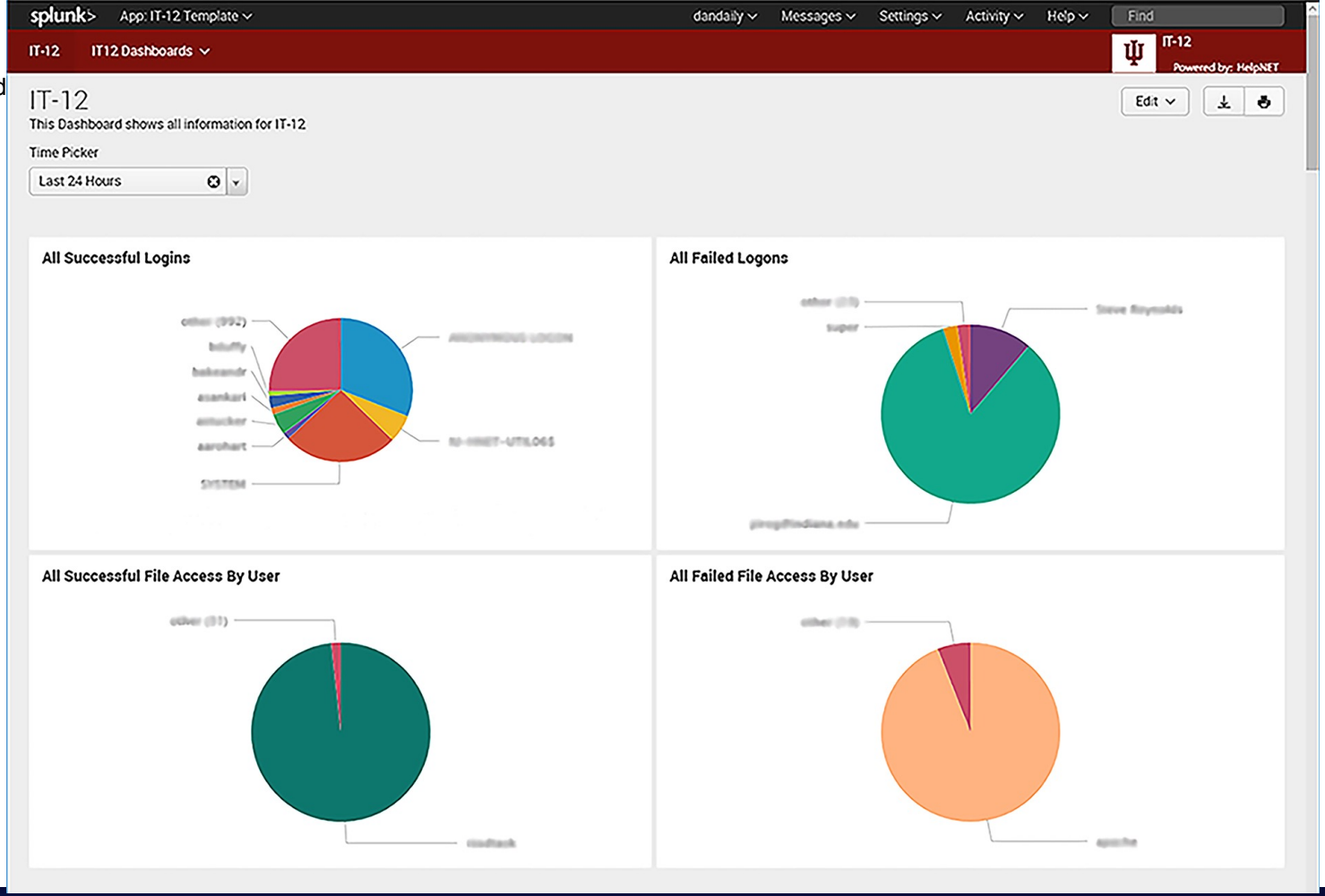
Saved Searches



Splunk Defaults Are Inclusive

```
dispatchAs = [user|owner]
* When the saved search is dispatched via the "saved/searches/{name}/dispatch"
  endpoint, this setting controls, what user that search is dispatched as.
* This setting is only meaningful for shared saved searches.
* When dispatched as user it will be executed as if the requesting user owned
  the search.
* When dispatched as owner it will be executed as if the owner of the search
  dispatched it no matter what user requested it.
* Defaults to owner
```

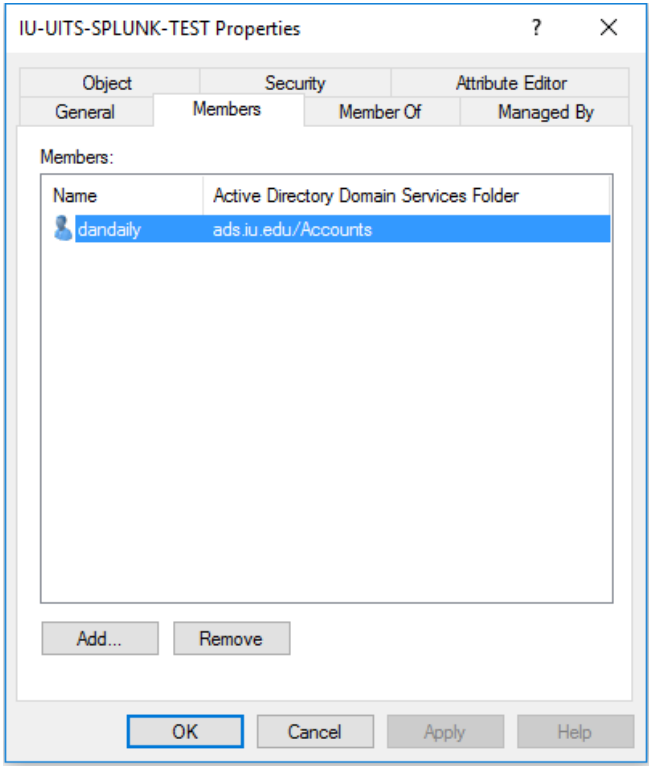
ind



Application Layer Configuration

Authorize.conf
[role_test]
search = enabled
srchIndexesAllowed = *

Authentication.conf
[roleMap_iuhelpnet01]
test = IU-UITS-SPLUNK-TEST



F.B.I. TERMINAL

This is a secured and monitored Federal Goverment system. Unauthorized access is strictly prohibited. All activity is fully monitored. Individuals who attempt to gain unauthorized access or attempt any modification of information on this sytem is subject to criminal prosecution. All persons who are hereby notified that use of this sytem constitutes concent to monitoring and auditing.

Search Bar

Rest API

curl -u 'dandaily' "https://localhost:8089/services/search/jobs/export?output_mode=json&search=search “index %3D_internal|head”"

With Application security alone…

Search bar and Rest API =

Security Best Practices For A Multitenant Environment

Best Practices

Use single sign-on and/or Active Directory Authentications

Manage configurations through Deployer/Deployment server

Configure Dual Layer Security

Dual Security Layer Configuration

Authentication.conf
[roleMap_iuhelpnet01]
test = IU-UITS-SPLUNK-TEST

Authorize.conf
[role_test]
srchIndexesAllowed = _internal

local.meta
[]
access = read : [admin, test, splunk-system-role],
write : [admin]
export = none

[reports]
access = read : [admin, test, splunk-system-role],
write : [admin]
export = none

Extra Security Options

Additional Security

Scope access search bar via Application Security

Scope user capabilities through authorize.conf

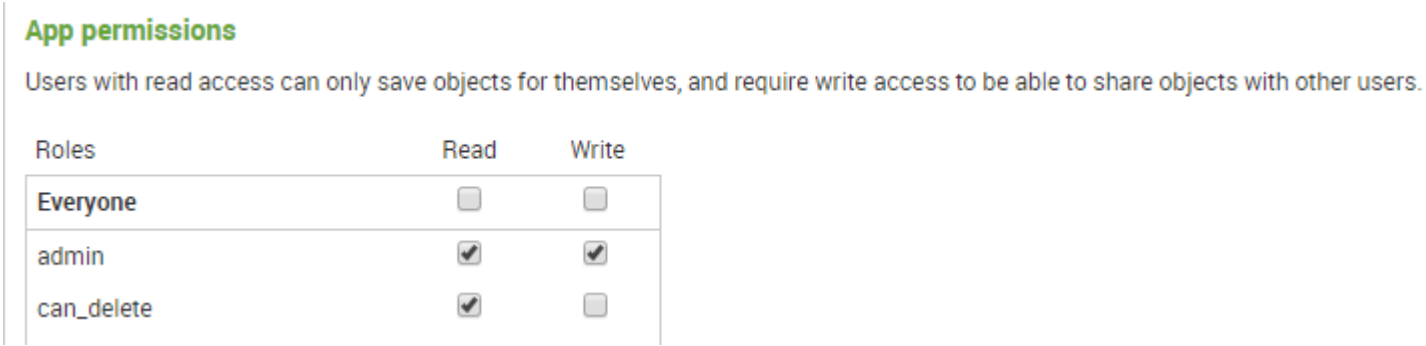
Search Bar Access

Benefits:

Limits the number of searches ran in the environment

Easier to scale architecture

Limit poorly formed searches



Limit User Access

Authorize.conf

[role_hnet]
search = enabled
srchIndexesAllowed = iuhnet
srchIndexesDefault = iuhnet
srchJobsQuota = 12
srchDiskQuota = 750
rest_properties_get = enabled
accelerate_search = enabled

THANK YOU

splunk>